

PCT

ORGANISATION MONDIALE DE LA PROPRIÉTÉ INTELLECTUELLE
Bureau international

EXPRESS MAIL MAILING LABEL

No. EL280660416US

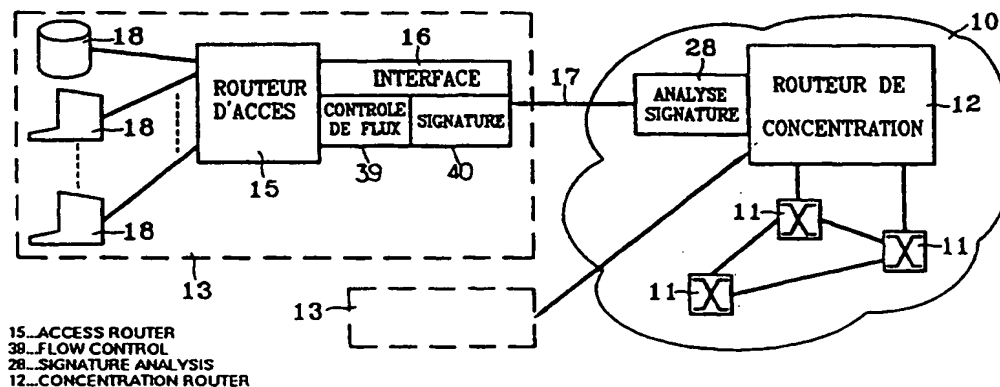


DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets ⁶ : H04L		A2	(11) Numéro de publication internationale: WO 00/36778
			(43) Date de publication internationale: 22 juin 2000 (22.06.00)
(21) Numéro de la demande internationale: PCT/FR99/03097 (22) Date de dépôt international: 10 décembre 1999 (10.12.99) (30) Données relatives à la priorité: 98/15756 14 décembre 1998 (14.12.98) FR (71) Déposant (pour tous les Etats désignés sauf US): NETCEN- TRENX [FR/FR]; 9, boulevard Detolle, Résidence Olympia, F-14000 Caen (FR). (72) Inventeur; et (75) Inventeur/Déposant (US seulement): HERSENT, Olivier [FR/FR]; 9, boulevard Detolle, Résidence Olympia, F-14000 Caen (FR). (74) Mandataires: LOISEL, Bertrand etc.; Cabinet Plasseraud, 84, rue d'Amsterdam, F-75440 Paris Cedex 09 (FR).		(81) Etats désignés: CA, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Publiée <i>Sans rapport de recherche internationale, sera republiée dès réception de ce rapport.</i>	

(54) Title: METHOD FOR TRANSPORTING PACKETS BETWEEN A SUBSCRIBER'S INSTALLATION ACCESS INTERFACE AND A SHARED NETWORK, AND ACCESS INTERFACE IMPLEMENTING SAID METHOD

(54) Titre: PROCEDE DE TRANSPORT DE PAQUETS ENTRE UNE INTERFACE D'ACCES D'UNE INSTALLATION D'ABONNE ET UN RESEAU PARTAGE, ET INTERFACE D'ACCES METTANT EN OEUVRE UN TEL PROCEDE



(57) Abstract

The invention concerns an access interface (16) performing control operations on packet flows transmitted to the concentrating router (12) as part of a contract between the subscriber and a manager of the shared network (10). After performing the control operations concerning a packet to be transmitted, the interface access transmits said packet to the concentrating router with a signature based on a secret shared with the concentrating router, authenticating that the packet has been subjected to the control operations.

(57) Abrégé

L'interface d'accès (16) procède à des opérations de contrôle sur des flux de paquets émis vers le routeur de concentration (12), dans le cadre d'un contrat entre l'abonné et un gestionnaire du réseau partagé (10). Après avoir procédé aux opérations de contrôle vis-à-vis d'un paquet à émettre, l'interface d'accès émet ce paquet vers le routeur de concentration avec une signature basée sur un secret partagé avec le routeur de concentration, authentifiant que le paquet a été soumis aux opérations de contrôle.

Best Available Copy

ONLY FOR INFORMATION

Codes used to identify the PCT member States on the flyleaves of the brochures in which international applications made under the PCT are published.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia-Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	Former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Vietnam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Ivory Coast	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

PROCÉDÉ DE TRANSPORT DE PAQUETS ENTRE UNE INTERFACE
D'ACCÈS D'UNE INSTALLATION D'ABONNÉ ET UN RÉSEAU PARTAGÉ,
ET INTERFACE D'ACCÈS METTANT EN ŒUVRE UN TEL PROCÉDÉ

La présente invention concerne les réseaux de transmission par
5 paquets. Elle s'applique notamment, mais non exclusivement, aux réseaux
partagés fonctionnant selon le protocole Internet (IP).

La mise en œuvre de l'invention intervient dans le cadre des relations
contractuelles entre un fournisseur d'accès au réseau partagé et ses clients. Le
fournisseur dispose, pour le raccordement des installations de ses clients, d'un
10 ou plusieurs routeurs de concentration du réseau partagé. Des lignes de
transmission relient ce routeur de concentration aux interfaces d'accès des
installations des clients, qui peuvent être des interfaces de routeurs d'accès de
réseaux privés.

On désigne ici par fonctions de « police » divers traitements ou
15 contrôles effectués au niveau d'une interface du réseau sur des flux de
données qui la traversent. A titre d'exemples non limitatifs, on peut citer le
comptage des paquets échangés entre une adresse de source et une adresse
de destination données, l'attribution de priorités à certains paquets, des
traductions d'adresse, la destruction sélective de certains paquets, etc.

Ces fonctions de police peuvent s'inscrire dans un cadre contractuel
entre un abonné (client) et un gestionnaire du réseau (fournisseur de services).
Cela peut par exemple être le cas de fonctions relatives à la facturation, au
contrôle de débit, aux autorisations d'accès à certains sites reliés au réseau, à
la mise en œuvre de protocoles de réservation tels que RSVP,.... Elles
25 peuvent également s'inscrire dans le cadre de l'organisation interne d'un
réseau public ou privé, par exemple pour contrôler certains accès.

Habituellement, les fonctions de police relevant du cadre contractuel
entre le fournisseur d'accès et ses clients sont mises en œuvre au niveau des
interfaces de raccordement du routeur de concentration. Ce routeur héberge
30 des logiciels de contrôle des flux qui circulent sur ses différentes interfaces.
Les paquets ayant certaines adresses ou ports de provenance ou de
destination sont comptés, filtrés, réagencés... selon le type de service offert.
Du fait du nombre élevé d'installations susceptibles d'être reliées au routeur de
concentration et de la variété de services qui peuvent être rendus pour ces
35 installations, les différents contrôles de flux à appliquer peuvent augmenter

considérablement la complexité du routeur. Cet inconvénient est d'autant plus sensible que des traitements de plus en plus divers sont demandés par les clients ou requis par les nouveaux protocoles de réservation.

5 D'autre part, cette organisation n'est pas souple pour le client qui souhaite faire évoluer certaines caractéristiques du service qui lui est offert. Il doit pour cela s'adresser à son fournisseur pour que celui-ci effectue les changements requis au niveau de son routeur de concentration.

10 Un but de la présente invention est de proposer un mode de fonctionnement du réseau qui permette la prise en compte d'une grande diversité de contrôles de flux sans se traduire par une augmentation excessive de la complexité des routeurs de concentration, et avec une relative souplesse de configuration.

15 L'invention propose ainsi un procédé de transport de paquets entre une interface d'accès d'une installation d'abonné et un routeur de concentration d'un réseau partagé, dans lequel l'interface d'accès procède à des opérations de contrôle sur des flux de paquets émis vers le routeur de concentration, dans le cadre d'un contrat entre l'abonné et un gestionnaire du réseau partagé. Après avoir procédé aux opérations de contrôle vis-à-vis d'un paquet à émettre, l'interface d'accès émet ce paquet vers le routeur de concentration
20 avec une signature basée sur un secret partagé avec le routeur de concentration, authentifiant que le paquet a été soumis aux opérations de contrôle.

De préférence, l'obtention de la signature et certaines au moins des opérations de contrôle sont réalisées au sein d'un même circuit intégré, sans
25 accès physique immédiatement en amont de l'obtention de la signature.

Les contrôles de flux relevant du cadre contractuel entre le gestionnaire du réseau et l'abonné sont ainsi décentralisés, ce qui évite que le routeur de concentration ait à assumer toute la diversité des opérations requises par les différents abonnements. Le mécanisme de signature des
30 paquets garantit au gestionnaire du réseau que l'abonné, qui dispose dans ses locaux de l'interface d'accès, ne lui envoie pas de paquets qui n'auraient pas été soumis aux opérations de contrôle de flux, c'est-à-dire qui auraient contourné les fonctions de police et de facturation.

35 Le procédé donne lieu à une architecture distribuée de l'accès et de la concentration, qui est bien adaptée pour prendre en compte les augmentations de trafic et de diversité de services qu'entraîneront les applications futures.

L'abonné bénéficie en outre d'une plus grande souplesse pour définir dynamiquement les caractéristiques de son abonnement. Il lui suffit d'intervenir au niveau de l'interface d'accès dont il dispose. Il peut d'autre part définir les fonctions de police relevant du cadre contractuel avec le fournisseur d'accès sur la même plate-forme que les autres fonctions de police qu'il utilise pour l'organisation interne de son installation, ce qui simplifie son organisation.

Un autre aspect de la présente invention se rapporte à une interface d'accès pour relier un routeur d'accès d'une installation d'abonné à un routeur de concentration d'un réseau partagé, comprenant des moyens de contrôle des flux de paquets émis vers le routeur de concentration, dans le cadre d'un contrat entre l'abonné et un gestionnaire du réseau partagé, et des moyens de signature recevant les paquets délivrés par les moyens de contrôle de flux et produisant des paquets signés émis vers le routeur de concentration, chaque paquet signé comportant une signature basée sur un secret partagé avec le routeur de concentration, authentifiant que le paquet a été soumis aux moyens de contrôle de flux.

D'autres particularités et avantages de la présente invention apparaîtront dans la description ci-après d'exemples de réalisation non limitatifs, en référence aux dessins annexés, dans lesquels :

- la figure 1 est un schéma d'un réseau où l'invention peut être mise en œuvre ;
- la figure 2 est un schéma synoptique d'un routeur d'accès d'une installation privée de ce réseau ;
- la figure 3 est un schéma synoptique d'un dispositif de traitement de flux faisant partie d'une interface du routeur de la figure 2 ; et
- la figure 4 est un graphe de traitements élémentaires assurés par le dispositif de la figure 3.

La figure 1 montre un réseau partagé de grande étendue (WAN) comportant un certain nombre de routeurs et commutateurs interconnectés 11,12. On considère ici le cas où le réseau partagé 10 fonctionne selon le protocole IP. Un certain nombre des routeurs sont des routeurs de concentration 12 auxquels sont reliées des installations privées 13.

Une installation privée d'abonné 13 est typiquement reliée au réseau partagé 10 au moyen d'un routeur d'accès 15 dont l'une des interfaces 16 est reliée à une ligne 17 de transmission depuis et vers le routeur de concentration 12. Le routeur d'accès 15 peut être relié à d'autres routeurs de l'installation

privée 13 ou à des serveurs ou terminaux 18 de cette installation, au moyen d'autres interfaces non représentées sur la figure 1.

La figure 2 montre un exemple d'architecture du routeur d'accès 15. L'interface extérieure 16, ainsi que les interfaces 20,21 avec le reste de l'installation privée 13, sont reliées au cœur du routeur consistant en un moteur d'acheminement de paquets 22 (« packet forwarding engine »). Le moteur d'acheminement 22 achemine les paquets d'une interface vers une autre sur la base des champs d'adresse et de port contenus dans les en-têtes des paquets conformément au protocole IP et à ses éventuelles extensions (TCP, UDP,...), en se reportant à des tables de routage.

Certaines des interfaces du routeur d'accès 15 sont pourvues, dans l'un seulement ou dans les deux sens de transmission, de dispositifs de traitement, ou processeurs de flux, 24,25 assurant des fonctions de police. Dans l'exemple illustratif de la figure 2, le dispositif 24 équipe l'interface extérieure 16 dans le sens sortant, et le dispositif 25 équipe une autre interface 20 dans le sens entrant.

Le routeur d'accès est supervisé par une unité de gestion 26 pouvant consister en un micro-ordinateur ou une station de travail qui exécute un logiciel de routage servant notamment à configurer la table de routage du moteur d'acheminement 22 et les processeurs de flux 24,25 et à échanger avec eux des informations de contrôle ou de protocole. Ces commandes et échanges se font par l'intermédiaire d'une interface logicielle de programmation (API) appropriée.

La plupart des logiciels de routage et d'acheminement de paquets existants sont facilement disponibles dans l'environnement Unix, mais leur performance est habituellement limitée à cause des interruptions fréquentes du système d'exploitation. Il est beaucoup plus rapide d'utiliser un système d'exploitation en temps réel tel que VxWorks, mais cela complique la mise en place du logiciel de routage.

Le rôle des processeurs de flux 24,25 est d'assister le système d'exploitation non-temps réel (tel qu'Unix), sur la base duquel fonctionne l'unité de gestion 26, dans les tâches complexes de manipulation des flux qui requièrent des performances en temps réel (acheminement, filtrage, chiffrement...). Ces processeurs mettent en œuvre un certain nombre d'outils de manipulation des flux qui peuvent être reliés dynamiquement suivant toute combinaison pour effectuer la tâche requise. Cette configuration peut être

effectuée à travers le système d'exploitation Unix par appel des fonctions d'API, ce qui facilite largement la mise en place de nouvelles fonctionnalités par le programmeur.

Comme illustré schématiquement par la figure 1, l'une des tâches effectuées par le processeur de flux 24 de l'interface extérieure 16 du routeur d'accès 15 consiste à émettre chaque paquet vers le routeur de concentration 12 en lui adjoignant une signature numérique (bloc 40). Cette signature atteste que les paquets en question ont été soumis aux autres opérations de contrôle de flux (bloc 39) effectuées par le processeur 24.

L'interface correspondante 28 du routeur de concentration 12 comporte un module d'analyse des paquets reçus sur la ligne 17 afin de s'assurer de la présence de la signature.

Cette technique de signature permet avantageusement de décentraliser les opérations de contrôle de flux nécessaires aux relations contractuelles entre le gestionnaire du routeur de concentration 12, qui fournit le service de raccordement au réseau partagé 10, et les abonnés dont les installations 13 sont reliées à ce routeur de concentration 12. Dans les réalisations classiques, ces opérations de contrôle de flux sont effectuées au niveau du routeur de concentration. Il en résulte une complexité considérable du routeur de concentration lorsqu'il est raccordé à d'assez nombreuses installations privées, et un manque de souplesse pour les abonnés lorsque des modifications sont requises.

Le fait d'effectuer ces opérations de contrôle de flux au niveau des routeurs d'accès 15 procure à cet égard une grande souplesse. La signature des paquets garantit alors au fournisseur de service que la ligne 17 ne lui envoie pas de paquets valides qui échapperaient au cadre contractuel avec l'abonné. Si un tel paquet venait à apparaître, l'interface 28 du routeur de concentration 12 l'éliminerait simplement après avoir constaté l'absence de la signature adéquate.

Diverses méthodes classiques peuvent être utilisées pour construire et analyser la signature des paquets, sur la base d'un secret partagé entre les routeurs 12 et 15. La signature peut notamment avoir la forme d'un mot de code ajouté au contenu du paquet, et calculé sur la base de tout ou partie de ce contenu et d'une clé secrète, le calcul étant effectué à l'aide d'une fonction extrêmement difficile à inverser pour récupérer la clé secrète. On peut ainsi utiliser une technique de hachage du contenu du paquet, ou d'une partie

seulement de ce contenu, par exemple un hachage MD5 (voir R. Rivest, RFC 1231, « The MD5 Message Digest Algorithm »).

On peut également utiliser une méthode de chiffrement pour former la signature des paquets. Le contenu du paquet est alors chiffré à l'aide d'une clé privée, l'interface 28 du routeur de concentration assurant le déchiffrement correspondant à l'aide d'une clé publique ou privée. Les paquets non chiffrés, ou chiffrés au moyen d'une mauvaise clé sont alors détruits au niveau de l'interface 28.

En option, on peut prévoir que l'interface 28 du routeur de concentration signe également les paquets qu'elle émet sur la ligne 17, et que l'interface 16 du routeur d'accès vérifie cette signature pour s'assurer de la validité des paquets reçus.

La figure 3 montre l'organisation d'un processeur de flux 24 ou 25 d'une interface du routeur d'accès 15.

Le processeur de flux reçoit une séquence de paquets entrants 30 comportant chacun un en-tête 31 conformément au protocole IP, et délivre une séquence de paquets sortants 32 ayant un en-tête 33 après avoir effectué certains traitements élémentaires dont la nature dépend des flux de données concernés.

Les paquets entrants 30 sont rangés dans une mémoire de paquets 35 organisée en pile de type premier entré – premier sorti (FIFO). Chaque paquet est fourni à la mémoire 35 avec une étiquette de traitement 36. L'étiquette de traitement a initialement une valeur déterminée (0 dans l'exemple représenté) pour les paquets entrants 30.

Le processeur de flux est supervisé par une unité 37 qui coopère avec une table 38 permettant d'associer un module de traitement particulier à chaque valeur de l'étiquette de traitement. Dans l'exemple simplifié représenté sur la figure 3, le processeur de flux comporte un ensemble de cinq modules de traitement M1-M5 opérant des traitements élémentaires de nature différente.

Après l'exécution d'un traitement élémentaire, l'unité de supervision 37 consulte la mémoire de paquets 35. Si celle-ci n'est pas vide, un paquet en est extrait suivant l'organisation FIFO. L'unité de supervision 37 consulte la table 38 pour déterminer quel module de traitement correspond à l'étiquette de ce paquet. L'unité 37 active alors le module en question pour qu'il effectue le traitement élémentaire correspondant. Dans certains cas, ce traitement

élémentaire peut entraîner une modification du contenu du paquet, notamment de son en-tête.

On comprendra que l'« extraction » du paquet à laquelle il est fait référence est une extraction au sens logique de la mémoire FIFO. Le paquet n'est pas nécessairement enlevé de la mémoire. Les adresses des paquets dans la mémoire 35 peuvent être gérées de façon classique au moyen de pointeurs pour respecter l'organisation FIFO. Le module de traitement activé peut disposer simplement de l'adresse du paquet courant pour effectuer les lectures, analyses, modifications ou suppressions requises le cas échéant.

Le premier module de traitement M1, associé à l'étiquette initiale 0, est un module de filtrage qui analyse les champs d'adresse et/ou de définition de protocole, et/ou de port de l'en-tête IP des paquets. A l'aide d'une table d'association T1, le module de filtrage M1 délivre une seconde étiquette de traitement qui identifie un enchaînement de traitements élémentaires qui devront ensuite être effectués sur le paquet. Après avoir déterminé la seconde étiquette de traitement pour le paquet extrait de la mémoire 35, le module de filtrage M1 range à nouveau le paquet dans la mémoire 35, avec la seconde étiquette de traitement. Le traitement élémentaire suivant sera alors exécuté au moment où le paquet sera de nouveau extrait de la mémoire.

Le module M2 est un module de comptage des paquets relatifs à certains flux. Dans le cas de la table d'association 38 représentée sur la figure 3, ce module M2 est appelé pour les étiquettes de traitement 2 et 4. Lorsqu'il traite un paquet, le module M2 incrémente un compteur avec le nombre d'octets du paquet, ou encore avec la valeur 1 dans le cas d'un compteur de paquets. Le compteur peut être sécurisé, notamment s'il sert à la facturation de l'abonné par le gestionnaire du réseau 10. Dans le cas d'un compteur sécurisé, des requêtes sont régulièrement faites au fournisseur d'accès pour obtenir des crédits de transmission, les paquets considérés étant détruits si le crédit est épuisé.

Le module M3 de la figure 3 est un module de gestion de priorités. Dans le cas de la table d'association 38 représentée sur la figure 3, ce module M3 est appelé pour l'étiquette de traitement 3. Le module M3 opère sur le champ TOS ("Type Of Service") de l'en-tête IP des paquets. Le TOS est utilisé dans le réseau pour gérer des priorités d'acheminement afin de fournir une certaine qualité de service sur certaines liaisons. Le champ TOS peut être changé selon des tables préenregistrées. Ces tables peuvent être définies

sous le contrôle du fournisseur d'accès pour éviter que des paquets soient transmis avec une priorité élevée de façon inappropriée, ce qui pourrait perturber le réseau.

5 Le traitement élémentaire effectué en dernier sur un paquet de la mémoire 35 est soit sa destruction (module M4 activé par l'étiquette 8), soit sa remise vers la sortie du processeur de flux (module M5 activé par l'étiquette 5 ou 9). Le module M4 peut être utilisé pour détruire des paquets ayant une certaine destination et/ou une certaine provenance.

10 Les modules M2 et M3, qui ne terminent pas les traitements à assurer pour un paquet (sauf cas de destruction), fonctionnent chacun avec une table de traduction d'étiquette T2,T3. Cette table de traduction désigne, pour l'étiquette de traitement extraite de la mémoire 35 avec le paquet courant, une autre étiquette de traitement désignant le traitement élémentaire suivant à assurer. Le traitement élémentaire assuré par ce module M2 ou M3 se termine
15 par la mise en association du paquet avec cette autre étiquette de traitement et la réinjection du paquet ainsi traité dans la mémoire 35.

C'est ainsi qu'on peut effectuer des combinaisons de traitements très variées sur les différents flux de données traversant le processeur.

20 La figure 4 montre un exemple simplifié correspondant aux tables 38,T1-T3 représentées sur la figure 3. Le paquet entrant 30, associé à la première étiquette 0 est d'abord soumis au filtrage opéré par le module M1.

Dans le cas particulier considéré, le processeur de flux 24 compte les paquets émis depuis une adresse source AS1 vers une adresse de destination AD1 et un port P1, et modifie le champ TOS de ces paquets avant de les
25 délivrer sur la ligne 17, ce qui correspond à la branche supérieure du graphe de la figure 4. D'autre part, le processeur de flux 24 compte les paquets issus d'une adresse de source AS2 vers un port P2 avant de les détruire, ce qui correspond à la branche inférieure de la figure 4. Les autres paquets sont simplement délivrés vers la ligne 17. La valeur par défaut (9) de l'étiquette de
30 traitement retournée par le module M1 désigne donc simplement le module de sortie M5. Si le module M1 détecte dans le paquet extrait de la mémoire 35 la combinaison AS1, AD1, P1 dans les champs d'adresse et de port pertinents, il retourne le paquet avec l'étiquette de traitement 2. Si les valeurs AS2, P2 sont détectées dans les champs d'adresse et de port, c'est l'étiquette 4 qui est
35 retournée avec le paquet.

Ces étiquettes 2 et 4 correspondent toutes deux au module de

comptage M2. L'étiquette va également désigner pour ce module l'adresse mémoire du compteur devant être incrémenté. La table T2 avec laquelle fonctionne le module M2 permettra en fin de traitement d'effectuer le renvoi vers le module suivant à activer (M3 désigné par l'étiquette 3 pour les paquets dont le TOS doit être changé, M4 désigné par l'étiquette 8 pour les paquets à détruire).

Le module M3 reçoit des paquets avec l'étiquette de traitement 3, et les retourne avec l'étiquette 9 après avoir opéré la modification requise du champ TOS.

10 A partir de cet exemple simplifié, on voit que le processeur de flux permet, à partir de l'identification d'un flux par le module de filtrage M1, d'effectuer diverses combinaisons de traitements élémentaires d'une manière relativement simple et rapide.

Un avantage principal de cette façon de procéder est la souplesse des opérations de configuration du processeur de flux. Les tables 38, T1-T3 qui définissent un graphe quelconque de traitements élémentaires, tel que celui représenté sur la figure 4, peuvent être construites de manière relativement simple et avec une faible contrainte de temps réel au moyen de l'unité de gestion 36 à travers l'API. Il en est de même pour les informations permettant aux modules M1-M5 d'effectuer leurs traitements élémentaires (description des comptages à opérer par le module M2, façon de changer les champs TOS par le module M3, ...).

Dans la pratique, le processeur de flux pourra comprendre divers modules de traitement autres que ceux représentés à titre d'exemple sur les figures 3 et 4, suivant les besoins de chaque installation particulière (par exemple, module de gestion des files d'attente de sortie, module de traduction d'adresses, ...).

La fonction de signature des paquets émis, décrite précédemment, peut faire partie du traitement élémentaire assuré par le module de sortie M5. Dans une réalisation typique du routeur d'accès, le processeur de flux 24 sera inclus dans un circuit intégré d'application spécifique (ASIC) organisé autour d'un cœur de microcontrôleur. Cette réalisation permet qu'il n'y ait aucun accès physique entre les modules de contrôle de flux 39 (du moins ceux qui concernent les relations entre l'abonné et le gestionnaire du réseau 10) et le module M5 qui se charge de la signature des paquets, correspondant au bloc 40 de la figure 1. Ceci améliore la sécurité de la liaison du point de vue du

gestionnaire du réseau.

REVENDICATIONS

1. Procédé de transport de paquets entre une interface d'accès (16) d'une installation d'abonné (13) et un routeur de concentration (12) d'un réseau partagé (10), caractérisé en ce que l'interface d'accès procède à des
5 opérations de contrôle sur des flux de paquets émis vers le routeur de concentration, dans le cadre d'un contrat entre l'abonné et un gestionnaire du réseau partagé, et en ce qu'après avoir procédé aux opérations de contrôle vis-à-vis d'un paquet à émettre, l'interface d'accès émet ce paquet vers le routeur de concentration avec une signature basée sur un secret partagé avec le
10 routeur de concentration, authentifiant que le paquet a été soumis aux opérations de contrôle.
2. Procédé selon la revendication 1, dans lequel la signature consiste en un mot de code ajouté au contenu du paquet.
3. Procédé selon la revendication 2, dans lequel ledit mot de code est
15 calculé par une technique de hachage d'une partie au moins du contenu du paquet, faisant intervenir le secret partagé.
4. Procédé selon la revendication 1, dans lequel la signature consiste en un chiffrement du contenu du paquet à l'aide d'une clé privée formant ledit secret partagé.
- 20 5. Procédé selon l'une quelconque des revendications 1 à 4, dans lequel l'obtention de la signature et certaines au moins des opérations de contrôle sont réalisées au sein d'un même circuit intégré, sans accès physique immédiatement en amont de l'obtention de la signature.
6. Interface d'accès pour relier un routeur d'accès (15) d'une
25 installation d'abonné (13) à un routeur de concentration (12) d'un réseau partagé (10), caractérisée en ce qu'elle comprend des moyens (39) de contrôle de flux de paquets émis vers le routeur de concentration, dans le cadre d'un contrat entre l'abonné et un gestionnaire du réseau partagé, et des moyens de signature (40) recevant les paquets délivrés par les moyens de contrôle de flux
30 et produisant des paquets signés émis vers le routeur de concentration, chaque paquet signé comportant une signature basée sur un secret partagé

avec le routeur de concentration, authentifiant que le paquet a été soumis aux moyens de contrôle de flux.

7. Interface selon la revendication 6, dans laquelle la signature consiste en un mot de code ajouté au contenu du paquet.

5 8. Interface selon la revendication 7, dans laquelle ledit mot de code est calculé par les moyens de signature (40) par une technique de hachage d'une partie au moins du contenu du paquet, faisant intervenir le secret partagé.

9. Interface selon la revendication 6, dans laquelle la signature
10 consiste en un chiffrement du contenu du paquet à l'aide d'une clé privée formant ledit secret partagé.

10. Interface selon l'une quelconque des revendications 6 à 9, dans laquelle les moyens de signature (40) et une partie au moins des moyens de contrôle de flux (39) font partie d'un même circuit intégré, sans accès physique
15 entre les moyens de contrôle de flux et les moyens de signature.

1/3

FIG. 1

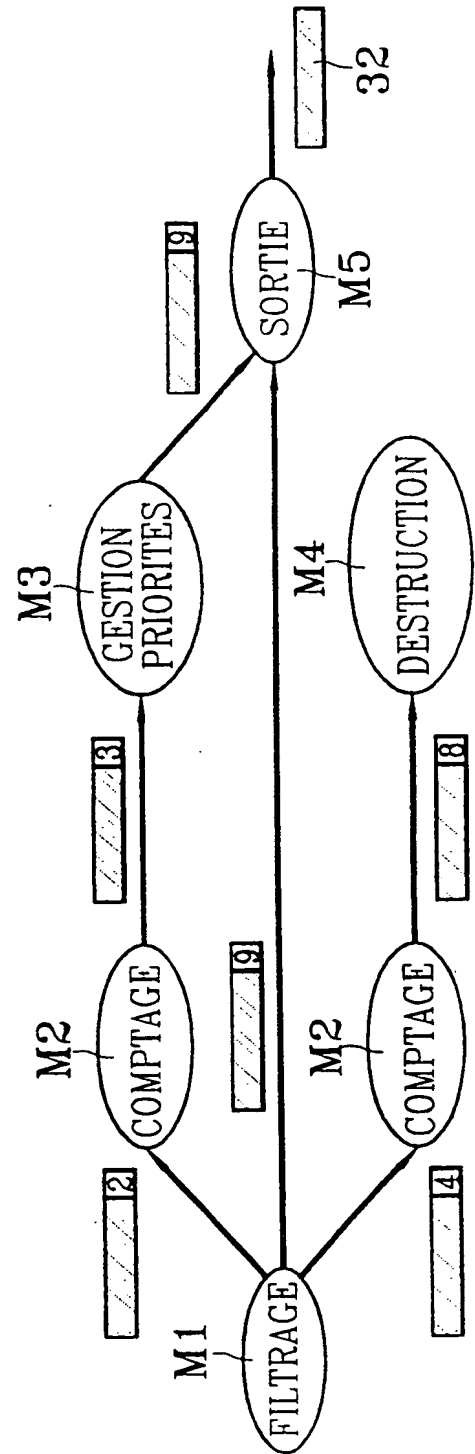
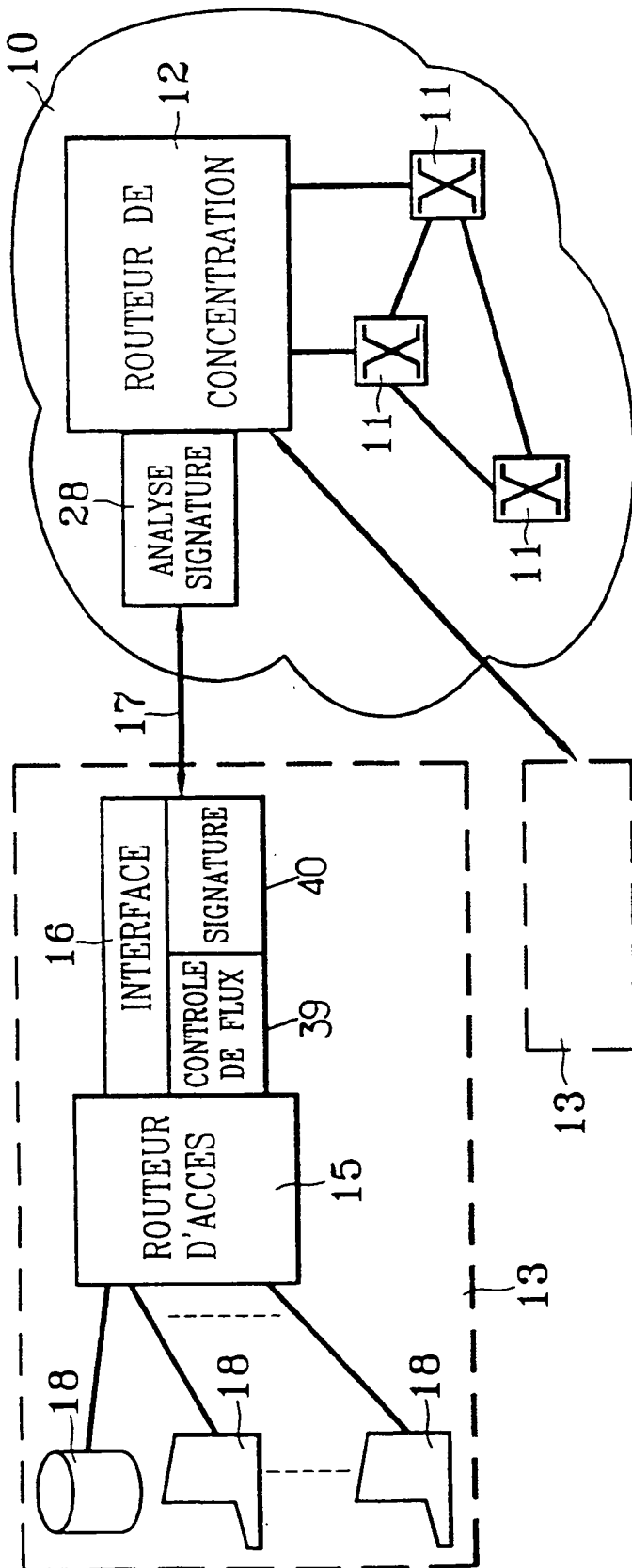
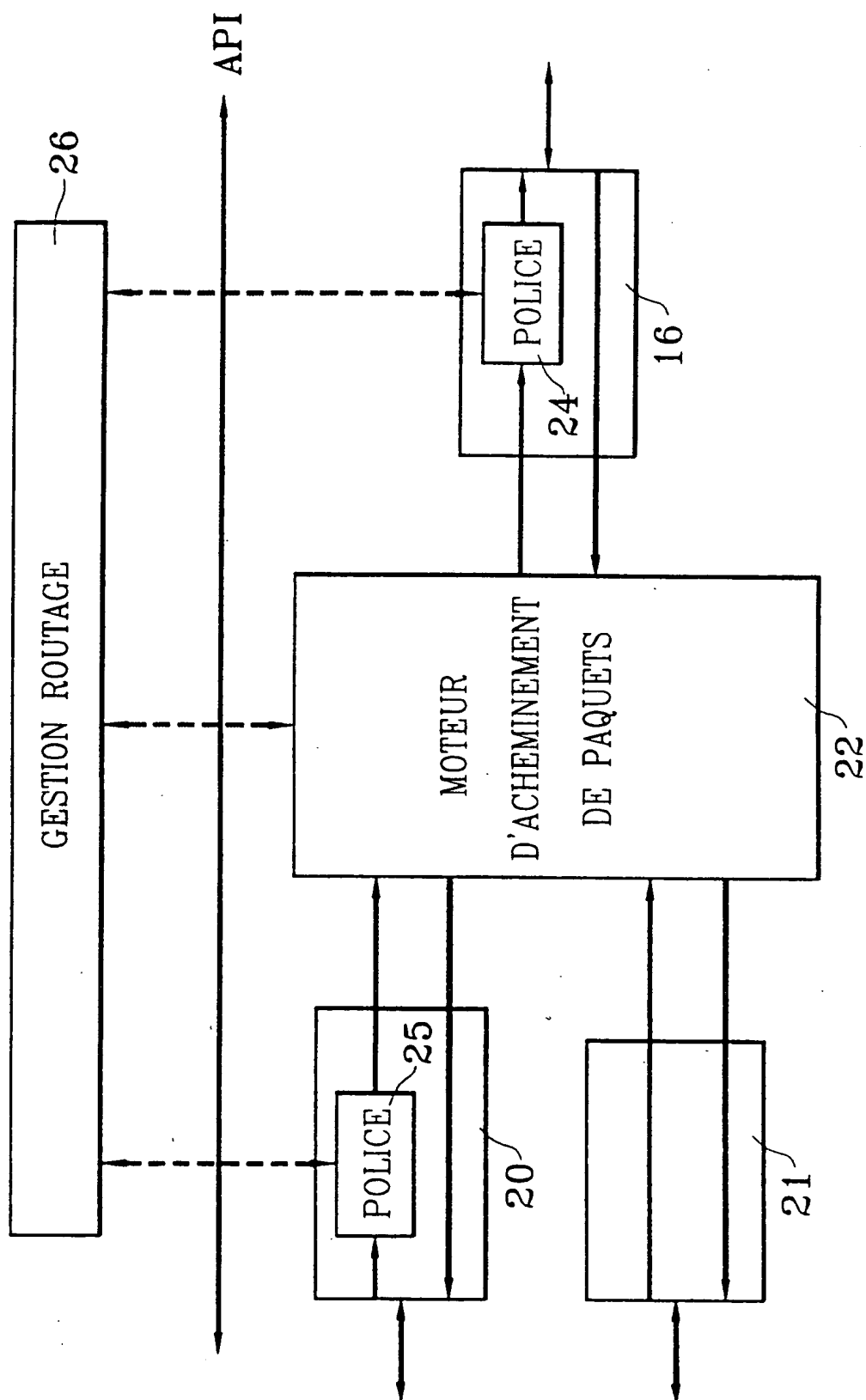
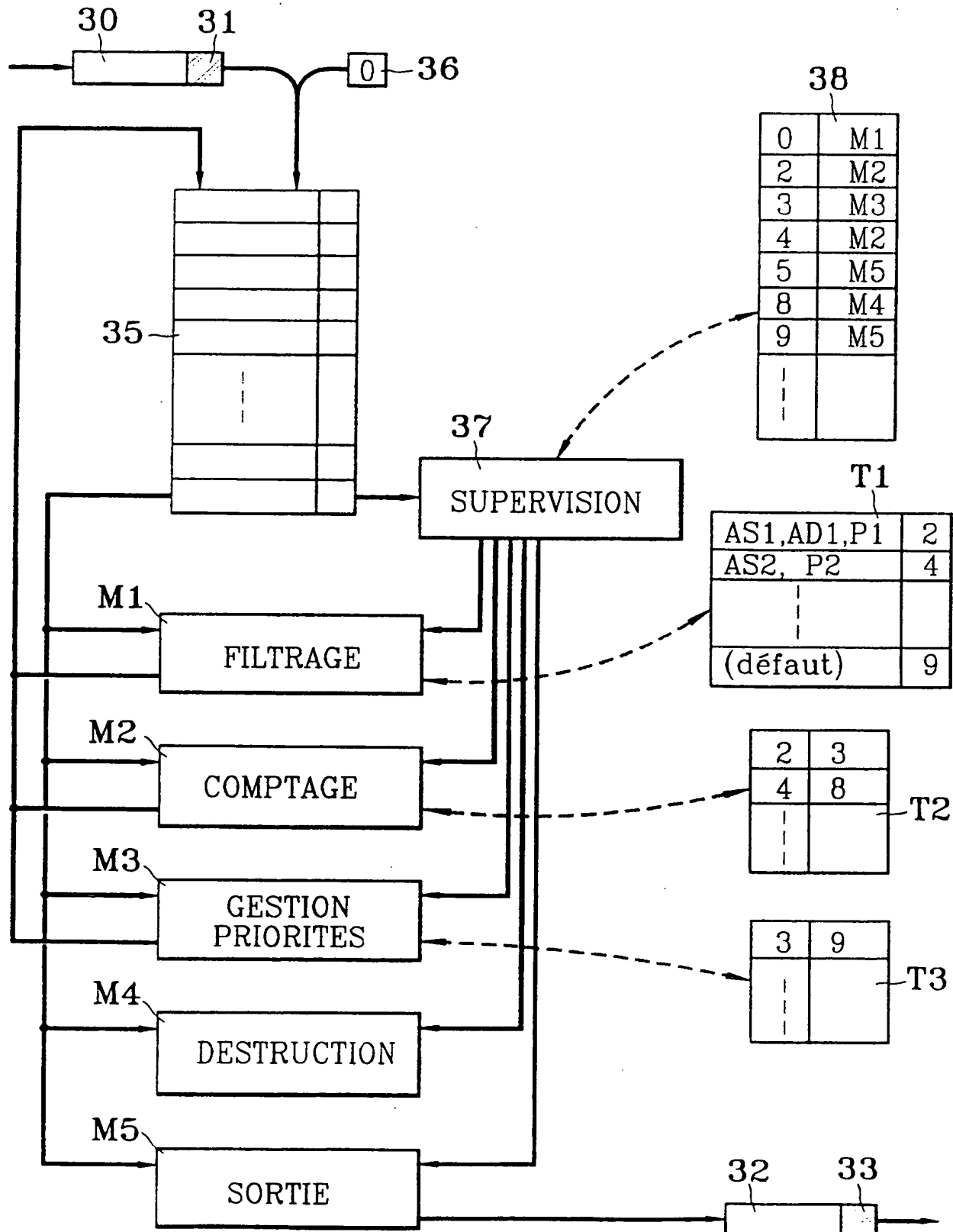


FIG. 4

FIG.2



3/3
FIG. 3



PCT

REQUÊTE

Le soussigné requiert que la présente demande internationale soit traitée conformément au Traité de coopération en matière de brevets.

Réserve Office récepteur

EXPRESS MAIL MAILING LABEL

Demande internationale n°

No. EL28060041605

Date du dépôt international

Nom de l'office récepteur et "Demande internationale PCT"

 Référence du dossier du déposant ou du mandataire (facultatif)
 (12 caractères au maximum) BCT990076/BLO

Cadre n° I TITRE DE L'INVENTION Procédé de transport de paquets entre une interface d'accès d'une installation d'abonné et un réseau partagé, et interface d'accès mettant en oeuvre un tel procédé.

Cadre n° II DÉPOSANT

Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'Etat où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)

NETCENTREX
 9, Boulevard Detolle
 Résidence Olympia
 14000 CAEN
 FRANCE

☐ Cette personne est aussi inventeur.

n° de téléphone

n° de télécopieur

n° de téléimprimeur

 Nationalité (nom de l'Etat) :
 FR

 Domicile (nom de l'Etat) :
 FR

 Cette personne est
 déposant pour :

☐ tous les États
 désignés

☒ tous les États désignés sauf
 les États-Unis d'Amérique

☐ les États-Unis d'Amérique
 seulement

☐ les États indiqués dans
 le cadre supplémentaire

Cadre n° III AUTRE(S) DÉPOSANT(S) OU (AUTRE(S)) INVENTEUR(S)

Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'Etat où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)

HERSENT Olivier
 9, Boulevard Detolle
 Résidence Olympia
 14000 CAEN
 FRANCE

Cette personne est :

☐ déposant seulement

☒ déposant et inventeur

☐ inventeur seulement
 (Si cette case est cochée,
 ne pas remplir la suite.)

 Nationalité (nom de l'Etat) :
 FR

 Domicile (nom de l'Etat) :
 FR

 Cette personne est
 déposant pour :

☐ tous les États
 désignés

☐ tous les États désignés sauf
 les États-Unis d'Amérique

☒ les États-Unis d'Amérique
 seulement

☐ les États indiqués dans
 le cadre supplémentaire

☐ D'autres déposants ou inventeurs sont indiqués sur une feuille annexe.

Cadre n° IV MANDATAIRE OU REPRÉSENTANT COMMUN; OU ADRESSE POUR LA CORRESPONDANCE

La personne dont l'identité est donnée ci-dessous est/ a été désignée pour agir au nom du ou des déposants auprès des autorités internationales compétentes, comme :

☒ mandataire

☐ représentant commun

Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays.)

LOISEL Bertrand - JACQUELIN Marc-Henri
 CABINET PLASSERAUD
 84 rue d'Amsterdam
 75440 PARIS CEDEX 09
 FRANCE

n° de téléphone

01 44 63 41 11

n° de télécopieur

01 42 80 01 59

n° de téléimprimeur

☐ Adresse pour la correspondance : cocher cette case lorsque aucun mandataire ni représentant commun n'est/ n'a été désigné et que l'espace ci-dessus est utilisé pour indiquer une adresse spéciale à laquelle la correspondance doit être envoyée.

Cadre n° V DESIGNATION D'ÉTAT

Les désignations suivantes sont faites conformément à la règle 4.9.a) (cocher les cases appropriées; une au moins doit l'être) :

Brevet régional

- ☐ AP Brevet ARIPO : GH Ghana, GM Gambie, KE Kenya, LS Lesotho, MW Malawi, SD Soudan, SL Sierra Leone, SZ Swaziland, UG Ouganda, ZW Zimbabwe et tout autre État qui est un État contractant du Protocole de Harare et du PCT
- ☐ EA Brevet eurasien : AM Arménie, AZ Azerbaïdjan, BY Bélarus, KG Kirghizistan, KZ Kazakhstan, MD République de Moldova, RU Fédération de Russie, TJ Tadjikistan, TM Turkménistan et tout autre État qui est un État contractant de la Convention sur le brevet eurasien et du PCT
- ☒ EP Brevet européen : AT Autriche, BE Belgique, CH et LI Suisse et Liechtenstein, CY Chypre, DE Allemagne, DK Danemark, ES Espagne, FI Finlande, FR France, GB Royaume-Uni, GR Grèce, IE Irlande, IT Italie, LU Luxembourg, MC Monaco, NL Pays-Bas, PT Portugal, SE Suède et tout autre État qui est un État contractant de la Convention sur le brevet européen et du PCT
- ☐ OA Brevet OAPI : BF Burkina Faso, BJ Bénin, CF République centrafricaine, CG Congo, CI Côte d'Ivoire, CM Cameroun, GA Gabon, GN Guinée, GW Guinée-Bissau, ML Mali, MR Mauritanie, NE Niger, SN Sénégal, TD Tchad, TG Togo et tout autre État qui est un État membre de l'OAPI et un État contractant du PCT (si une autre forme de protection ou de traitement est souhaitée, le préciser sur la ligne pointillée)

Brevet national (si une autre forme de protection ou de traitement est souhaitée, le préciser sur la ligne pointillée) :

- | | |
|--|---|
| <input type="checkbox"/> AE Émirats arabes unis | <input type="checkbox"/> LR Liberia |
| <input type="checkbox"/> AL Albanie | <input type="checkbox"/> LS Lesotho |
| <input type="checkbox"/> AM Arménie | <input type="checkbox"/> LT Lituanie |
| <input type="checkbox"/> AT Autriche | <input type="checkbox"/> LU Luxembourg |
| <input type="checkbox"/> AU Australie | <input type="checkbox"/> LV Lettonie |
| <input type="checkbox"/> AZ Azerbaïdjan | <input type="checkbox"/> MD République de Moldova |
| <input type="checkbox"/> BA Bosnie-Herzégovine | <input type="checkbox"/> MG Madagascar |
| <input type="checkbox"/> BB Barbade | <input type="checkbox"/> MK Ex-République yougoslave de Macédoine |
| <input type="checkbox"/> BG Bulgarie | |
| <input type="checkbox"/> BR Brésil | <input type="checkbox"/> MN Mongolie |
| <input type="checkbox"/> BY Bélarus | <input type="checkbox"/> MW Malawi |
| <input checked="" type="checkbox"/> CA Canada | <input type="checkbox"/> MX Mexique |
| <input type="checkbox"/> CH et LI Suisse et Liechtenstein | <input type="checkbox"/> NO Norvège |
| <input type="checkbox"/> CN Chine | <input type="checkbox"/> NZ Nouvelle-Zélande |
| <input type="checkbox"/> CU Cuba | <input type="checkbox"/> PL Pologne |
| <input type="checkbox"/> CZ République tchèque | <input type="checkbox"/> PT Portugal |
| <input type="checkbox"/> DE Allemagne | <input type="checkbox"/> RO Roumanie |
| <input type="checkbox"/> DK Danemark | <input type="checkbox"/> RU Fédération de Russie |
| <input type="checkbox"/> EE Estonie | <input type="checkbox"/> SD Soudan |
| <input type="checkbox"/> ES Espagne | <input type="checkbox"/> SE Suède |
| <input type="checkbox"/> FI Finlande | <input type="checkbox"/> SG Singapour |
| <input type="checkbox"/> GB Royaume-Uni | <input type="checkbox"/> SI Slovénie |
| <input type="checkbox"/> GD Grenade | <input type="checkbox"/> SK Slovaquie |
| <input type="checkbox"/> GE Géorgie | <input type="checkbox"/> SL Sierra Leone |
| <input type="checkbox"/> GH Ghana | <input type="checkbox"/> TJ Tadjikistan |
| <input type="checkbox"/> GM Gambie | <input type="checkbox"/> TM Turkménistan |
| <input type="checkbox"/> HR Croatie | <input type="checkbox"/> TR Turquie |
| <input type="checkbox"/> HU Hongrie | <input type="checkbox"/> TT Trinité-et-Tobago |
| <input type="checkbox"/> ID Indonésie | <input type="checkbox"/> UA Ukraine |
| <input type="checkbox"/> IL Israël | <input type="checkbox"/> UG Ouganda |
| <input type="checkbox"/> IN Inde | <input checked="" type="checkbox"/> US États-Unis d'Amérique |
| <input type="checkbox"/> IS Islande | |
| <input type="checkbox"/> JP Japon | <input type="checkbox"/> UZ Ouzbékistan |
| <input type="checkbox"/> KE Kenya | <input type="checkbox"/> VN Viet Nam |
| <input type="checkbox"/> KG Kirghizistan | <input type="checkbox"/> YU Yougoslavie |
| <input type="checkbox"/> KP République populaire démocratique de Corée | <input type="checkbox"/> ZA Afrique du Sud |
| | <input type="checkbox"/> ZW Zimbabwe |
| <input type="checkbox"/> KR République de Corée | Cases réservées pour la désignation d'États qui sont devenus parties au PCT après la publication de la présente feuille : |
| <input type="checkbox"/> KZ Kazakhstan | <input type="checkbox"/> |
| <input type="checkbox"/> LC Sainte-Lucie | <input type="checkbox"/> |
| <input type="checkbox"/> LK Sri Lanka | <input type="checkbox"/> |

Déclaration concernant les désignations de précaution : outre les désignations faites ci-dessus, le déposant fait aussi conformément à la règle 4.9.b) toutes les désignations qui seraient autorisées en vertu du PCT, à l'exception de toute désignation indiquée dans le cadre supplémentaire comme étant exclue de la portée de cette déclaration. Le déposant déclare que ces désignations additionnelles sont faites sous réserve de confirmation et que toute désignation qui n'est pas confirmée avant l'expiration d'un délai de 15 mois à compter de la date de priorité doit être considérée comme retirée par le déposant à l'expiration de ce délai. (Pour confirmer une désignation, il faut déposer une déclaration contenant la désignation en question et payer les taxes de désignation et de confirmation. La confirmation doit parvenir à l'office récepteur dans le délai de 15 mois.)

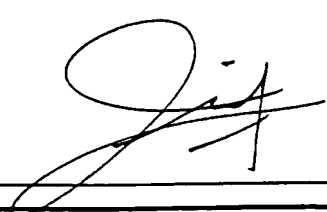
Cadre n° VI REVENDEICATION PRIORITÉ		<input type="checkbox"/> Les revendications de priorité sont indiquées dans le cadre supplémentaire.		
Date de dépôt de la demande antérieure (jour/mois/année)	Numéro de la demande antérieure	Lorsque la demande antérieure est une :		
		demande nationale : pays	demande régionale : * office régional	demande internationale : office récepteur
(1) 14 DECEMBRE 98 (14/12/1998)	98 15756	FRANCE		
(2)				
(3)				

☐ L'office récepteur est prié de préparer et de transmettre au Bureau international une copie certifiée conforme de la ou des demandes antérieures (seulement si la demande antérieure a été déposée auprès de l'office qui, aux fins de la présente demande internationale, est l'office récepteur) indiquées ci-dessus au(x) point(s) :

* Si la demande antérieure est une demande ARIPO, il est obligatoire d'indiquer dans le cadre supplémentaire au moins un pays partie à la Convention de Paris pour la protection de la propriété industrielle pour lequel cette demande antérieure a été déposée (régie 4.10.biii). Voir le cadre supplémentaire.

Cadre n° VII ADMINISTRATION CHARGÉE DE LA RECHERCHE INTERNATIONALE			
Choix de l'administration chargée de la recherche internationale (ISA) (si plusieurs administrations chargées de la recherche internationale sont compétentes pour procéder à la recherche internationale, indiquer l'administration choisie; le code à deux lettres peut être utilisé) :		Demande d'utilisation des résultats d'une recherche antérieure; mention de cette recherche (si une recherche antérieure a été effectuée par l'administration chargée de la recherche internationale ou demandée à cette dernière) :	
ISA/ EP		Date (jour/mois/année)	Numéro Pays (ou office régional)
		5/10/1999	FA 568520 FRANCE

Cadre n° VIII BORDEREAU: LANGUE DE DÉPÔT	
La présente demande internationale contient le nombre de feuilles suivant :	Le ou les éléments cochés ci-après sont joints à la présente demande internationale :
requête : 3	1. <input checked="" type="checkbox"/> feuille de calcul des taxes
description (sauf partie réservée au listage des séquences) : 10	2. <input type="checkbox"/> pouvoir distinct signé
revendications : 2	3. <input type="checkbox"/> copie du pouvoir général; numéro de référence, le cas échéant :
abrégé : 1	4. <input type="checkbox"/> explication de l'absence d'une signature
dessins : 3	5. <input type="checkbox"/> document(s) de priorité indiqué(s) dans le cadre n° VI au(x) point(s) :
partie de la description réservée au listage des séquences : _____	6. <input type="checkbox"/> traduction de la demande internationale en (langue) :
Nombre total de feuilles : 19	7. <input type="checkbox"/> indications séparées concernant des micro-organismes ou autre matériel biologique déposés
	8. <input type="checkbox"/> listage des séquences de nucléotides ou d'acides aminés sous forme déchiffrable par ordinateur
	9. <input checked="" type="checkbox"/> autres éléments (préciser) : COPIE DU RAPPORT DE RECHERCHE
Figure des dessins qui doit accompagner l'abrégé : 1	Langue de dépôt de la demande internationale : FRANCAISE

Cadre n° IX SIGNATURE DU DÉPOSANT OU DU MANDATAIRE	
À côté de chaque signature, indiquer le nom du signataire et, si cela n'apparaît pas clairement à la lecture de la requête, à quel titre l'intéressé signe.	
 Paris, le 10 décembre 1999 LOISEL Bertrand	

Réservé à l'office récepteur	
1. Date effective de réception des pièces supposées constituer la demande internationale :	2. Dessins : <input type="checkbox"/> reçus : <input type="checkbox"/> non reçus :
3. Date effective de réception, rectifiée en raison de la réception ultérieure, mais dans les délais, de documents ou de dessins complétant ce qui est supposé constituer la demande internationale :	
4. Date de réception, dans les délais, des corrections demandées selon l'article 11.2) du PCT :	
5. Administration chargée de la recherche internationale (si plusieurs sont compétentes) : ISA/	6. <input type="checkbox"/> Transmission de la copie de recherche différée jusqu'au paiement de la taxe de recherche.

Réservé au Bureau international	
Date de réception de l'exemplaire original par le Bureau international :	

TRAITE DE COOPERATION EN MATIERE DE BREVETS

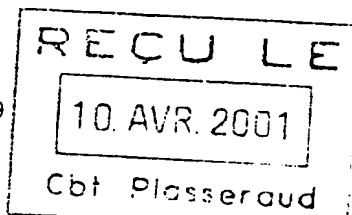
EXPRESS MAIL MAILING LABEL

Expéditeur: L'ADMINISTRATION CHARGÉE DE
L'EXAMEN PRÉLIMINAIRE INTERNATIONAL

No. EL280660416US

Destinataire:

LOISEL, B.
CABINET PLASSERAUD
84, rue d'Amsterdam
F-75440 PARIS Cedex 09
FRANCE



PCT

NOTIFICATION DE TRANSMISSION DU
RAPPORT D'EXAMEN PRÉLIMINAIRE
INTERNATIONAL
(règle 7.1 du PCT)
**CONFIRMATION
FAX-Bestätigung**

Date d'expédition
(jour/mois/année) 03.04.2001

Référence du dossier du déposant ou du mandataire
BCT990076/BLO

NOTIFICATION IMPORTANTE

Demande internationale No.
PCT/FR99/03097

Date du dépôt international (jour/mois/année)
10/12/1999

Date de priorité (jour/mois/année)
14/12/1998

Déposant
NETCENTREX et al.

1. Il est notifié au déposant que l'administration chargée de l'examen préliminaire international a établi le rapport d'examen préliminaire international pour la demande internationale et le lui transmet ci-joint, accompagné, le cas échéant, de ces annexes.

2. Une copie du présent rapport et, le cas échéant, de ses annexes est transmise au Bureau international pour communication à tous les offices élus.

3. Si tel ou tel office élu l'exige, le Bureau international établira une traduction en langue anglaise du rapport (à l'exclusion des annexes de celui-ci) et la transmettra aux offices intéressés.

4. RAPPEL

Pour aborder la phase nationale auprès de chaque office élu, le déposant doit accomplir certains actes (dépôt de traduction et paiement des taxes nationales) dans le délai de 30 mois à compter de la date de priorité (ou plus tard pour ce qui concerne certains offices) (article 39.1) (voir aussi le rappel envoyé par le Bureau international dans le formulaire PCT/IB/301).

Lorsqu'une traduction de la demande internationale doit être remise à un office élu, elle doit comporter la traduction de toute annexe du rapport d'examen préliminaire international. Il appartient au déposant d'établir la traduction en question et de la remettre directement à chaque office élu intéressé.

Pour plus de précisions en ce qui concerne les délais applicables et les exigences des offices élus, voir le Volume II du Guide du déposant du PCT.

Nom et adresse postale de l'administration chargée de l'examen préliminaire international

Office européen des brevets
D-80298 Munich
Tél. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Fonctionnaire autorisé

Ahrens, R

Tél. +49 89 2399-8136



TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)



Référence du dossier du déposant ou du mandataire BCT990076/BLO	POUR SUITE A DONNER voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR99/03097	Date du dépôt international (jour/mois/année) 10/12/1999	Date de priorité (jour/mois/année) 14/12/1998
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L29/06		
Déposant NETCENTREX et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.
2. Ce RAPPORT comprend 6 feuilles, y compris la présente feuille de couverture.
 - ☐ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

Ces annexes comprennent feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

- I ☒ Base du rapport
- II ☐ Priorité
- III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
- IV ☐ Absence d'unité de l'invention
- V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- VI ☐ Certains documents cités
- VII ☒ Irrégularités dans la demande internationale
- VIII ☐ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale 13/07/2000	Date d'achèvement du présent rapport 03.04.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international:  Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Dechmann, J-L N° de téléphone +49 89 2399 8826 

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR99/03097

I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)*):

Description, pages:

1-10 version initiale

Revendications, N°:

1-10 version initiale

Dessins, feuilles:

1/3-3/3 version initiale

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

- ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
- ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
- ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

- ☐ contenu dans la demande internationale, sous forme écrite.
- ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
- ☐ remis ultérieurement à l'administration, sous forme écrite.
- ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
- ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
- ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listage des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

**RAPPORT D'EXAMEN
PRÉLIMINAIRE INTERNATIONAL**

Demande internationale n° PCT/FR99/03097

- ☐ de la description, pages :
☐ des revendications, n^{os} :
☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

(Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui : Revendications 1-10
	Non : Revendications
Activité inventive	Oui : Revendications 1-10
	Non : Revendications
Possibilité d'application industrielle	Oui : Revendications 1-10
	Non : Revendications

**2. Citations et explications
voir feuille séparée**

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :
voir feuille séparée

V. Déclaration motivée selon la règle 66.2.a)ii) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

I

Les documents (D) suivants ont été pris en compte pour l'établissement du rapport d'examen préliminaire:

- D1: GRAY A: 'ROUTER ENCRYPTION MADE EASY - THE HARD WAY' DATA COMMUNICATIONS, vol. 26, no. 2, 1 février 1997 (1997-02-01), page 36, 38 XP000659573 ISSN: 0363-6399
- D2: GB-A-2 323 757
- D3: BRUNO L: 'SECURITY' DATA COMMUNICATIONS, vol. 27, no. 1, 1 janvier 1998 (1998-01-01), page 88, 90 XP000733531 ISSN: 0363-6399
- D4: MAKRIS J: 'LOCKING DOWN INTRANETS FROM AFAR-FOR LESS' DATA COMMUNICATIONS, vol. 27, no. 11, 1 août 1998 (1998-08-01), page 25/26 XP000782253 ISSN: 0363-6399
- D5: HEYWOOD P: 'PRODUCT LEADERS FILTERS WITHOUST FUSS' DATA COMMUNICATIONS, vol. 27, no. 8, 21 mai 1998 (1998-05-21), page 29/30 XP000755584 ISSN: 0363-6399
- D6: BAUSPIESS F ET AL: 'REQUIREMENTS FOR CRYPTOGRAPHIC HASH FUNCTIONS' COMPUTERS & SECURITY INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, vol. 11, no. 5, 1 septembre 1992 (1992-09-01), pages 427-437, XP000296996 ISSN: 0167-4048

II

La présente demande concerne les réseaux de transmission par paquets (Rev 1: procédé de transport; Rev 6: Interface d'accès). Elle s'applique notamment aux réseaux partagés fonctionnant selon le protocole Internet.

La mise en œuvre de l'invention intervient dans le cadre des relations contractuelles entre un fournisseur d'accès au réseau partagé et ses clients. Le fournisseur dispose pour le raccordement des installations de ses clients, d'un ou plusieurs routeurs de concentration du réseau partagé. Des lignes de transmission relient ce routeur de concentration aux interfaces d'accès des installations des clients qui peuvent être des interfaces de routeurs d'accès de réseaux privés.

Habituellement les fonctions de police relevant du cadre contractuel entre le fournisseur d'accès et ses clients sont mises en œuvre au niveau des interfaces de raccordement du routeur de concentration.

Ce routeur héberge des logiciels de contrôle des flux qui circulent sur ses différentes interfaces. Les paquets ayant certaines adresses ou ports de provenance ou de destination sont comptés, filtrés, réagencés selon le type de service offert.

Du fait du nombre élevé d'installations susceptibles d'être reliées au routeur de concentration et de la variété de services qui peuvent être rendus pour ces installations, les différents contrôles de flux à appliquer peuvent augmenter considérablement la **complexité du routeur**. D'autre part, cette organisation n'est pas souple pour le client qui souhaite faire évoluer certaines caractéristiques du service qui lui est offert. Il doit pour cela s'adresser à son fournisseur pour que celui-ci effectue les changements requis au niveau de son routeur de concentration.

Le but de la présente invention est donc de proposer un mode de fonctionnement du réseau qui permette la prise en compte d'une grande diversité de contrôles de flux sans se traduire par une augmentation excessive de la complexité des routeurs de concentration, et avec une relative souplesse de configuration.

L'invention propose ainsi un procédé de transport de paquets entre une interface d'accès d'une installation d'abonné et un routeur de concentration d'un réseau partagé, dans lequel l'interface d'accès procède à des opérations de contrôle sur des flux de paquets émis vers le routeur de concentration, dans le cadre d'un contrat entre l'abonné et un gestionnaire du réseau partagé. Après avoir procédé aux opérations de contrôle vis-à-vis d'un paquet à émettre, l'interface d'accès émet ce paquet vers le routeur de concentration avec une signature basée sur un secret partagé avec le routeur de concentration, authentifiant que le paquet a été soumis aux opérations de contrôle.

Les contrôles de flux relevant du cadre contractuel entre le gestionnaire du réseau et

l'abonné sont ainsi **décentralisés**, ce qui évite que le routeur de concentration ait à assumer toute la diversité des opérations requises par les différents abonnements. Le mécanisme de signature des paquets garantit au gestionnaire du réseau que l'abonné, qui dispose dans ses locaux de l'interface d'accès, ne lui envoie pas de paquets qui n'auraient pas été soumis aux opérations de contrôle de flux, c'est-à-dire qui auraient contourné les fonctions de police et de facturation.

Le procédé donne lieu à une **architecture distribuée** de l'accès et de la concentration, qui est bien adaptée pour prendre en compte les augmentations de trafic et de diversité de services qu'entraîneront les applications futures.

L'abonné bénéficie en outre d'une plus grande souplesse pour définir dynamiquement les caractéristiques de son abonnement. Il lui suffit d'intervenir au niveau de l'interface d'accès dont il dispose. Il peut d'autre part définir les fonctions de police relevant du cadre contractuel avec le fournisseur d'accès sur la même plate-forme que les autres fonctions de police qu'il utilise pour l'organisation interne de son installation, ce qui simplifie son organisation.

Une telle solution n'est ni décrite ni dérivée des documents cités et une activité inventive est reconnue. Les revendications 1-10 satisfont donc les exigences de l'Article 33(3) PCT.

VII. Irrégularités dans la demande internationale

1. Si le Demandeur a connaissance d'un document représentant l'état de la technique tel qu'il le décrit à l'introduction de la description page 1 ("...Habituellement les fonctions de police relevant du cadre contractuel entre le fournisseur d'accès et ses clients sont mises en oeuvre au niveau des interfaces de raccordement du routeur de concentration..."), il lui est demandé d'identifier ce document conformément à la Règle 5.1(a)(ii) du PCT.

Dans le cas contraire, le Demandeur est prié de mentionner et de brièvement analyser les documents D1 à D4 dans la partie introductive de la description.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No

P R 99/03097

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L29/06

EXPRESS MAIL MAILING LABEL

No. EL280660416US

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	GRAY A: "ROUTER ENCRYPTION MADE EASY - THE HARD WAY" DATA COMMUNICATIONS, vol. 26, no. 2, 1 février 1997 (1997-02-01), page 36, 38 XP000659573 ISSN: 0363-6399 le document en entier ----	1,6
A	BRUNO L: "SECURITY" DATA COMMUNICATIONS, vol. 27, no. 1, 1 janvier 1998 (1998-01-01), page 88, 90 XP000733531 ISSN: 0363-6399 le document en entier ----- -/--	2-4,7-9



Voir la suite du cadre C pour la fin de la liste des documents



Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

- "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- "E" document antérieur, mais publié à la date de dépôt international ou après cette date
- "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"Z" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

6 novembre 2000

Date d'expédition du présent rapport de recherche internationale

14/11/2000

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Carnerero Álvaro, F

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	MAKRIS J: "LOCKING DOWN INTRANETS FROM AFAR-FOR LESS" DATA COMMUNICATIONS, vol. 27, no. 11, 1 août 1998 (1998-08-01), page 25/26 XP000782253 ISSN: 0363-6399 le document en entier ----	1-10
A	HEYWOOD P: "PRODUCT LEADERS FILTERS WITHOUT FUSS" DATA COMMUNICATIONS, vol. 27, no. 8, 21 mai 1998 (1998-05-21), page 29/30 XP000755584 ISSN: 0363-6399 le document en entier ----	1-10
A	BAUSPIESS F ET AL: "REQUIREMENTS FOR CRYPTOGRAPHIC HASH FUNCTIONS" COMPUTERS & SECURITY INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, vol. 11, no. 5, 1 septembre 1992 (1992-09-01), pages 427-437, XP000296996 ISSN: 0167-4048 page 427 -page 429 ----	2,3,7,8
A	GB 2 323 757 A (IBM) 30 septembre 1998 (1998-09-30) abrégé page 7, ligne 1 -page 10, ligne 4 figure 4 -----	1-10

Renseignements relatifs aux membres de familles de brevets

PR 99/03097

Formulaire PCT/ISA/210 (annexe familles de brevets) (juillet 1992)

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

Assistant Commissioner for Patents
United States Patent and Trademark
Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

en sa qualité d'office élu

Date d'expédition (jour/mois/année)

01 août 2000 (01.08.00)

Demande internationale no

PCT/FR99/03097

Référence du dossier du déposant ou du mandataire

BCT990076/BLO

Date du dépôt international (jour/mois/année)

10 décembre 1999 (10.12.99)

Date de priorité (jour/mois/année)

14 décembre 1998 (14.12.98)

Déposant

HERSENT, Olivier

1. L'office désigné est avisé de son élection qui a été faite:



dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

13 juillet 2000 (13.07.00)



dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection



a été faite



n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur: (41-22) 740.14.35

Fonctionnaire autorisé

Alejandro HENNING

no de téléphone: (41-22) 338.83.38

Translation
09/868/51

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

RECEIVED
JAN 24 2002
Technology Center 2100

Applicant's or agent's file reference BCT990076/BLO	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/FR99/03097	International filing date (day/month/year) 10 December 1999 (10.12.99)	Priority date (day/month/year) 14 December 1998 (14.12.98)
International Patent Classification (IPC) or national classification and IPC H04L 29/06		
Applicant NETCENTREX		

<p>1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.</p> <p>2. This REPORT consists of a total of <u>6</u> sheets, including this cover sheet.</p> <p><input type="checkbox"/> This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).</p> <p>These annexes consist of a total of _____ sheets.</p>	
<p>3. This report contains indications relating to the following items:</p> <p>I <input checked="" type="checkbox"/> Basis of the report</p> <p>II <input type="checkbox"/> Priority</p> <p>III <input type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</p> <p>IV <input type="checkbox"/> Lack of unity of invention</p> <p>V <input checked="" type="checkbox"/> Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</p> <p>VI <input type="checkbox"/> Certain documents cited</p> <p>VII <input checked="" type="checkbox"/> Certain defects in the international application</p> <p>VIII <input type="checkbox"/> Certain observations on the international application</p>	

Date of submission of the demand 13 July 2000 (13.07.00)	Date of completion of this report 03 April 2001 (03.04.2001)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR99/03097

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

- ☐ the international application as originally filed.
- ☒ the description, pages 1-10, as originally filed,
 pages _____, filed with the demand,
 pages _____, filed with the letter of _____,
 pages _____, filed with the letter of _____.
- ☒ the claims, Nos. 1-10, as originally filed,
 Nos. _____, as amended under Article 19,
 Nos. _____, filed with the demand,
 Nos. _____, filed with the letter of _____,
 Nos. _____, filed with the letter of _____.
- ☒ the drawings, sheets/fig 1/3-3/3, as originally filed,
 sheets/fig _____, filed with the demand,
 sheets/fig _____, filed with the letter of _____,
 sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR 99/03097

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-10	YES
	Claims		NO
Inventive step (IS)	Claims	1-10	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-10	YES
	Claims		NO

2. Citations and explanations

I

The following documents (D) have been taken into account to establish the preliminary examination report:

- D1: CRAY A: 'ROUTER ENCRYPTION MADE EASY - THE HARD WAY' DATA COMMUNICATIONS, vol.26, no.2, 1 February 1997 (1997-02-01), page 36, 38
XP000659573 ISSN: 0363-6399
- D2: GB-A-2 323 757
- D3: BRUNO L: 'SECURITY' DATA COMMUNICATIONS, vol.27, no.1, 1 January 1998 (1998-01-01), page 88, 90
XP000733531 ISSN: 0363-6399
- D4: MAKRIS J: 'LOCKING DOWN INTRANETS FROM AFAR-FOR LESS' DATA COMMUNICATIONS, vol.27, no.11, 1 August 1998 (1998-08-01), page 25/26 XP000782253
ISSN: 0363-6399
- D5: HEYWOOD P: 'PRODUCT LEADERS FILTERS WITHOUT FUSS' DATA COMMUNICATIONS, vol.27, no.8, 21 May 1998 (1998-05-21), page 29/30 XP000755584 ISSN: 0363-6399
- D6: BAUSPIESS F ET AL: 'REQUIREMENTS FOR CRYPTOGRAPHIC HASH FUNCTIONS' COMPUTERS & SECURITY INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF

COMPUTER SECURITY, vol.11, no.5, 1 September
1992 (1992-09-01), pages 427-437, XP000296996
ISSN: 0167-4048

II

The present application relates to packet transmission networks (Claim 1: transport method; Claim 6: Access interface). It is particularly applicable to shared networks operating according to Internet Protocol.

The invention applies to contractual relationships between a shared network access provider and its clients. The provider uses one or more shared network concentration routers for the connection of client installations. Transmission lines connect said concentration router to the access interfaces of the client installations, which may be interfaces of private network access routers. Generally, the policy functions relating to the agreement between the access provider and its clients are applied at the connection interfaces of the concentration router. Said router accommodates flow control software programs that run on different interfaces. Packets having certain origin or destination addresses or ports are counted, filtered, rearranged according to the type of service offered.

Because of the large number of installations that are likely to be connected to the concentration router and the variety of services that can be provided for these installations, the different flow controls to be applied can significantly increase **router complexity**. However, this organization is not flexible for the client who wishes to change certain features of the service offered. The client must therefore send a request to the provider

in order for the latter to make the necessary changes at the concentration router level.

The aim of the present invention is, therefore, to propose a method for operating the network that enables the recognition of a large variety of flow controls without involving an excessive increase in concentration router complexity, and with a relatively flexible configuration. The invention therefore proposes a method for transporting packets between an access interface of a subscriber installation and a concentration router of a shared network, in which the access interface carries out control operations over the flow of packets sent to the concentration router, as part of an agreement between the subscriber and a manager of the shared network. After carrying out the control operations relating to a packet to be sent, the access interface sends this package towards the concentration router with a signature based on a secret shared with the concentration router, authenticating that the packet has been subjected to the control operations.

The flow controls relating to the agreement between the network manager and the subscriber are therefore **decentralized**, preventing the concentration router from taking over all of the various operations required by the different subscriptions. The signature mechanism of the packets provides the guarantee to the network manager that the subscriber, who has on premises the access interface, does not send packets that have not been subjected to the flow control operations, that is to say, that have bypassed the policy and billing functions.

The method leads to a **distributed network architecture** for access and concentration, which is well designed for managing the increases in traffic and variety of services that future applications will involve.

The subscriber benefits, additionally, from a greater flexibility for dynamically defining the subscription features. The subscriber only needs to take action at the level of the access interface that he/she is using. The subscriber can also define the policy functions of the agreement with the access provider on the same platform as the other policy functions that the subscriber uses for the internal organization of his/her installation, which simplifies organization.

Such a solution is neither described nor derivable from the cited documents and an inventive step is recognized. Claims 1-10 therefore meet the requirements of PCT Article 33(3).

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1. If the Applicant has knowledge of a document describing the prior art as it is described in the introduction of the description on page 1 ("...Generally, the policy functions relating to the agreement between the access provider and its clients are implemented at the connection interfaces of the concentration router..."), the applicant is asked to identify this document in accordance with PCT Rule 5.1(a)(ii).

If this is not the case, the Applicant is asked to mention and to briefly analyze documents D1 to D4 in the introductory part of the description.

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.